10/665,338

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	"20030039355"	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:16
L2	1	"20020041685"	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:17
L3	1114	380/37 or 380/42	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:17
L4	108	3 and "s box"	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:18
L5	96	3 and "s-box"	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:18
L6	108	5 or 4	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:18
L7	13	6 and encrypt$3 and shift and "round key"	US-PGPUB; USPAT	OR	OFF	2007/01/04 08:19
L8	66	"s box" and encrypt$3 and shift and "round key"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/01/04 08:19
L9	10236	stein.inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/01/04 08:20
L10	36	9 and yosef	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/01/04 08:21
L11	18	10 and kablotsky	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/01/04 08:21

Please Scan

Terms used **s box** and **encrypt$3** and **shift** and **round key** Found **58** of **193,448**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 58 Result page: **1** 2 3 next

Relevance scale

1 Reconfigurable architectures: REDEFIS: a system with a redefinable instruction set processor

Victor M. GOULART FERREIRA, Lovic GAUTHIER, Takayuki KANDO, Takuma MATSUO, Toshihiko HASHINAGA, Kazuaki MURAKAMI

August 2006 **Proceedings of the 19th annual symposium on Integrated circuits and systems design SBCCI '06**

Publisher: ACM Press

Full text available: pdf(930.50 KB) Additional Information: full citation, abstract, references, index terms

The growing complexity and production cost of processor-based systems have imposed big constraints in SoC design of new systems. GPPs and ASICs are unable to fit the tight performance or power constraints, or too complex to design in short TAT/TTM. REDEFIS is a HW/SW design platform for high level, efficient implementation of ASIPs/engines for SoC systems. It is composed of a reconfigurable instruction-set processor, capable to redefine its ISA according to the user application written in high l ...

Keywords: ISA customization, SoC, dynamically reconfigurable processor, high performance, low power

2 Concurrent error detection of fault-based side-channel cryptanalysis of 128-bit symmetric block ciphers

Ramesh Karri, Kaijie Wu, Piyush Mishra, Yongkook Kim

June 2001 **Proceedings of the 38th conference on Design automation**

Publisher: ACM Press

Full text available: pdf(260.32 KB) Additional Information: full citation, abstract, references, index terms

Fault-based side channel cryptanalysis is very effective against symmetric and asymmetric encryption algorithms. Although straightforward hardware and time redundancy based concurrent error detection (CED) architectures can be used to thwart such attacks, they entail significant overhead (either area or performance). In this paper we investigate systematic approaches to low-cost, low-latency CED for symmetric encryption algorithms based on the inverse relationship that exists between encryp ...

3 Security processor design: A configurable AES processor for enhanced security

Chih-Pin Su, Chia-Lung Horng, Chih-Tsun Huang, Cheng-Wen Wu

January 2005 **Proceedings of the 2005 conference on Asia South Pacific design automation ASP-DAC '05**

Publisher: ACM Press
Full text available: pdf(413.10 KB) Additional Information: full citation, abstract, references

We propose a configurable AES processor for extended-security communication. The proposed architecture can provide up to 2^{19} different AES block cipher schemes within a reasonable hardware cost. Data can be encrypted not only with secret keys and initial vectors, but also by different block ciphers during the communication. A novel on-the-fly key expansion design is also proposed for 128-, 192-, and 256-bit keys. Our unified hardware can run both the original AES algorithm and the ext ...

4 Applications: A methodology to implement block ciphers in reconfigurable hardware and its application to fast and compact AES RIJNDAEL

François-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, Jean-Didier Legat
February 2003 **Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays**
Publisher: ACM Press
Full text available: pdf(236.87 KB) Additional Information: full citation, abstract, references, citings, index terms

Reprogrammable devices such as Field Programmable Gate Arrays (FPGA's) are highly attractive options for hardware implementations of encryption algorithms and this report investigates a methodology to efficiently implement block ciphers in CLB-based FPGA's. Our methodology is applied to the new Advanced Encryption Standard RIJNDAEL and the resulting designs offer better performances than previously published in literature. We propose designs that unroll the 10 AES rounds and pipeline them in ord ...

Keywords: AES RIJNDAEL, FPGA, cryptography, high encryption rates, reconfigurable hardware

5 Embedded security and reliability: Methodology for attack on a Java-based PDA

C. H. Gebotys, B. A. White
October 2006 **Proceedings of the 4th international conference on Hardware/software codesign and system synthesis CODES+ISSS '06**
Publisher: ACM Press
Full text available: pdf(1.10 MB) Additional Information: full citation, abstract, references, index terms

Although mobile Java code is frequently executed on many wireless devices, the susceptibility to electromagnetic (EM) attacks is largely unknown. If analysis of EM waves emanating from the wireless device during a cryptographic computation does leak sufficient information, it may be possible for an attacker to reconstruct the secret key. Possession of the secret cryptographic key would render all future wireless communications insecure and cause further potential problems such as identity theft. ...

Keywords: embedded system

6 Embedded applications: AES and the cryptonite crypto processor

Dino Oliva, Rainer Buchty, Nevin Heintze
October 2003 **Proceedings of the 2003 international conference on Compilers, architecture and synthesis for embedded systems**
Publisher: ACM Press
Full text available: pdf(346.09 KB) Additional Information: full citation, abstract, references, index terms

CRYPTONITE is a programmable processor tailored to the needs of crypto algorithms. The design of CRYPTONITE was based on an in-depth application analysis in which standard crypto algorithms (AES, DES, MD5, SHA-1, etc) were distilled down to their core functionality. We describe this methodology and use AES as a central example. Starting

with a functional description of AES, we give a high level account of how to implement AES efficiently in hardware, and present several novel optimizations (whic ...

Keywords: AES, architecture, cryptography, high-bandwidth, high-speed, processor, round key generation, software implementation

7 Advances in design-for-testability methods: Secure scan: a design-for-test architecture for crypto chips

Bo Yang, Kaijie Wu, Ramesh Karri
June 2005 **Proceedings of the 42nd annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(234.65 KB) Additional Information: full citation, abstract, references, index terms

Scan-based Design-for-Test (DFT) is a powerful testing scheme, but it can be used to retrieve the secrets stored in a crypto chip thus compromising its security. On one hand, sacrificing security for testability by using traditional scan-based DFT restricts its use in privacy sensitive applications. On the other hand, sacrificing testability for security by abandoning scan-based DFT hurts product quality. The security of a crypto chip comes from the small secret key stored in a few registers and ...

Keywords: crypto hardware, scan-based DFT, security, testability

8 VLSI design: A 2 Gb/s balanced AES crypto-chip implementation

F. K. Guürkaynak, A. Burg, N. Felber, W. Fichtner, D. Gasser, F. Hug, H. Kaeslin
April 2004 **Proceedings of the 14th ACM Great Lakes symposium on VLSI**
Publisher: ACM Press
Full text available: pdf(97.22 KB) Additional Information: full citation, abstract, references, index terms

We present a balanced 2 Gb/s en-/decryption ASIC realization of the AES algorithm that supports all standard operation modes and key lengths. Rather than optimizing only for throughput, special care is taken to balance the more involved decryption path with that of the encryption path using a number of high-level architectural and register transfer level optimizations. The fabricated en-/decryption core requires an active area of only 3.56 mm² (less than 120,000 gate equivalents) in a ...

Keywords: AES, ASIC implementation, rijndael

9 A Low Device Occupation IP to Implement Rijndael Algorithm

Alex Panato, Marcelo Barcelos, Ricardo Reis
March 2003 **Proceedings of the conference on Design, Automation and Test in Europe: Designers' Forum - Volume 2 DATE '03**
Publisher: IEEE Computer Society
Full text available: pdf(455.68 KB) Publisher Site Additional Information: full citation, abstract, index terms

This work presents a soft IP description of Rijndael, the Advanced Encryption Standard (AES) of National Institute of Standards and Technology (NIST). This Rijndael implementation run its symmetric cipher algorithm using a key size of 128 bits, mode called AES128. The focus here is to produce a low area IP achieving good performance. To do that, we propose a architecture using mixed bit size processing. The usage of memory has a significant decrease. The same methodology is used to implement thr ...

10 An FPGA implementation and performance evaluation of the Serpent block cipher

A. J. Elbirt, C. Paar
February 2000 **Proceedings of the 2000 ACM/SIGDA eighth international symposium on Field programmable gate arrays**
Publisher: ACM Press

Full text available: pdf(674.09 KB) Additional Information: full citation, abstract, references, citings, index terms

With the expiration of the Data Encryption Standard (DES) in 1998, the Advanced Eneryption Standard (AES) development process is well underway. It is hoped that the result of the AES process will be the specification of a new non-classified encryption algorithm that will have the global acceptance achieved by DES as well as the capability of long-term protection of sensitive information. The technical analysis used in determining which of the potential AES candidates will be selected as the ...

Keywords: FPGA, VHDL, algorithm-agility, block cipher, cryptography

11 Applications: A fully pipelined memoryless 17.8 Gbps AES-128 encryptor

Kimmo U. Järvinen, Matti T. Tommiska, Jorma O. Skyttä
February 2003 **Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays**
Publisher: ACM Press

Full text available: pdf(124.00 KB) Additional Information: full citation, abstract, references, citings, index terms

A fully pipelined implementation of the Advanced Encryption Standard encryption algorithm with 128-bit input and key length (AES-128) was implemented on Xilinx' Virtex-E and Virtex-II devices. The design is called SIG-AES-E and it implements the S-boxes combinatorially and thus requires no internal memory. It is concluded, that SIG-AES-E is faster than other published FPGA-based implementations of the AES-128 encryption algorithm.

Keywords: FPGA, advanced encryption standard (AES), pipelining

12 Application 2: A compact FPGA implementation of the hash function whirlpool

Norbert Pramstaller, Christian Rechberger, Vincent Rijmen
February 2006 **Proceedings of the internation symposium on Field programmable gate arrays FPGA'06**
Publisher: ACM Press

Full text available: pdf(240.32 KB) Additional Information: full citation, abstract, references, index terms

Recent breakthroughs in cryptanalysis of standard hash functions like SHA-1 and MD5 raise the need for alternatives. A credible alternative to for instance SHA-1 or the SHA-2 family of hash functions is Whirlpool. Whirlpool is a hash function that has been evaluated and approved by NESSIE and is standardized by ISO/IEC. To the best of our knowledge only one FPGA implementation of Whirlpool has been published to date. This implementation is designed for high throughput rates requiring a considera ...

Keywords: FPGA, compact hardware implementation, hash function, whirlpool

13 Computer architecture: A 3.84 gbits/s AES crypto coprocessor with modes of operation in a 0.18-μm CMOS technology

Alireza Hodjat, David D. Hwang, Bocheng Lai, Kris Tiri, Ingrid Verbauwhede
April 2005 **Proceedings of the 15th ACM Great Lakes symposium on VLSI**
Publisher: ACM Press

Full text available: pdf(283.76 KB) Additional Information: full citation, abstract, references, index terms

In this paper an AES crypto coprocessor that is fabricated using a 0.18-μm CMOS technology is presented. This crypto coprocessor performs the AES-128 encryption in both feedback and non-feedback modes of operation. A maximum throughput of 3.84 Gbits/s is achieved at a 330 MHz clock frequency for ECB, OFB, and CBC modes of operation. This crypto coprocessor can be programmed using the memory-mapped interface of an embedded CPU core and is tested using a LEON 32-bit (SPARC V8) processor in th ...

Keywords: ASIC, FPGA, VLSI, advanced encryption standard (AES), crypto-processor, cryptography, hardware architectures, security

14 Survey and benchmark of block ciphers for wireless sensor networks

Yee Wei Law, Jeroen Doumen, Pieter Hartel
February 2006 **ACM Transactions on Sensor Networks (TOSN)**, Volume 2 Issue 1
Publisher: ACM Press
Full text available: pdf(354.39 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic algorithms play an important role in the security architecture of wireless sensor networks (WSNs). Choosing the most storage- and energy-efficient block cipher is essential, due to the facts that these networks are meant to operate without human intervention for a long period of time with little energy supply, and that available storage is scarce on these sensor nodes. However, to our knowledge, no systematic work has been done in this area so far. We construct an evaluation framew ...

Keywords: Sensor networks, block ciphers, cryptography, energy efficiency

15 Architectures for cryptography and security applications: High performance encryption cores for 3G networks

Tomás Balderas-Contreras, René Cumplido
June 2005 **Proceedings of the 42nd annual conference on Design automation**
Publisher: ACM Press
Full text available: pdf(869.33 KB) Additional Information: full citation, abstract, references, index terms

This paper presents two novel and high performance hardware architectures, implemented in FPGA technology, for the KASUMI block cipher; this algorithm lies at the core of the confidentiality and integrity algorithms defined for the Universal Mobile Telecommunication System (UMTS) standard. The first proposal is a pipelined design and the second implements an iterative approach. The throughput for these architectures turn out to be higher than the throughput achieved by other proposals.

Keywords: 3G, FPGA, KASUMI, UMTS security architecture

16 Systematic generation of cryptographically robust S-boxes

Jennifer Seberry, Xian-Mo Zhang, Yuliang Zheng
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.20 MB) Additional Information: full citation, abstract, references, index terms

Substitution boxes (S-boxes) are a crucial component of DES-like block ciphers. This research addresses problems with previous approaches towards constructing S-boxes, and proposes a new definition for the robustness of S-boxes to differential cryptanalysis, which is the most powerful cryptanalytic attack known to date. A novel method based on

group Hadamard matrices is developed to systematically generate S-boxes that satisfy a number of critical cryptographic properties. Among the propert ...

17 Secure and security systems: Satisfiability-based framework for enabling side-channel attacks on cryptographic software

Nachiketh R. Potlapally, Anand Raghunathan, Srivaths Ravi, Niraj K. Jha, Ruby B. Lee

March 2006 **Proceedings of the conference on Design, automation and test in Europe: Designers' forum DATE '06**

Publisher: European Design and Automation Association

Full text available: pdf(161.25 KB) Additional Information: full citation, abstract, references

Many electronic systems contain implementations of cryptographic algorithms in order to provide security. It is well known that cryptographic algorithms, irrespective of their theoretical strength, can be broken through weaknesses in their implementation. In particular, side-channel attacks, which exploit unintended information leakage from the implementation, have been established as a powerful way of attacking cryptographic systems. All side-channel attacks can be viewed as consisting of two p ...

18 Poster session 1: An FPGA design of AES encryption circuit with 128-bit keys

Hui Qin, Tsutomu Sasao, Yukihiro Iguchi

April 2005 **Proceedings of the 15th ACM Great Lakes symposium on VLSI**

Publisher: ACM Press

Full text available: pdf(238.43 KB) Additional Information: full citation, abstract, references, index terms

This paper addresses a pipelined partial rolling (PPR) architecture for the AES encryption. The key technique is the PPR architecture, which is suitable for FPGA implementation. Using the proposed architecture on the Altera Stratix EP1S20F780C5 FPGA, the AES-4SM achieves a throughput of 5.61 Gbps by using 20 M4Ks, and the AES-8SM achieves a throughput of 10.49 Gbps by using 40 M4Ks. Compared with the unrolling implementation that achieves a throughput of 20.48 Gbps by using 80 M4Ks on the same F ...

Keywords: AES encryption, FPGA, pipeline

19 Combinatorial sketching for finite programs

Armando Solar-Lezama, Liviu Tancau, Rastislav Bodik, Sanjit Seshia, Vijay Saraswat

October 2006 **ACM SIGOPS Operating Systems Review , ACM SIGPLAN Notices , ACM SIGARCH Computer Architecture News , Proceedings of the 12th international conference on Architectural support for programming languages and operating systems ASPLOS-XII**, Volume 40 , 41 , 34 Issue 5 , 11 , 5

Publisher: ACM Press

Full text available: pdf(314.21 KB) Additional Information: full citation, abstract, references, index terms

Sketching is a software synthesis approach where the programmer develops a partial implementation - a sketch - and a separate specification of the desired functionality. The synthesizer then completes the sketch to behave like the specification. The correctness of the synthesized implementation is guaranteed by the compiler, which allows, among other benefits, rapid development of highly tuned implementations without the fear of introducing bugs.We develop SKETCH, a language for finite programs ...

Keywords: SAT, sketching

20 Draft Proposed: American National Standard—Graphical Kernel System

Technical Committee X3H3 - Computer Graphics

February 1984 **ACM SIGGRAPH Computer Graphics**, Volume 18 Issue SI

Publisher: ACM Press
Full text available: pdf(16.07 MB) Additional Information: full citation

Results 1 - 20 of 58 Result page: **1** 2 3 next